Ollscoil na hÉireann, Gaillimh *GX_____*

National University of Ireland, Galway

Summer Examinations, 2010/2011

Exam Code(s)	4IF1 Bachelor of Science in Information Technology
Module Code(s)	CT437
Module(s)	Computer Security and Forensic Computing
Paper No.	1
External Examiner(s)	Prof. M. O'Boyle
Internal Examiner(s)	Prof. G. Lyons Dr. J. Duggan Dr. C. Mulvihill*
Instructions:	Answer any four questions. All questions will be marked equally.
Duration	3 hrs
No. of Answer Books	1
No. of Pages	1
Department(s)	Information Technology

1 (a) Explain what is meant by a 'security policy document' and outline three suitable components (6 marks)
(b) Risk analysis is important in security work. Explain what is meant by 'single loss expectancy' and 'annual loss expectancy' in this context (6 marks)
(c) Given the following three risk factors: flooding, lack of ID for employees, encrypted laptop theft, discuss how you might approach ranking them for the purposes of risk analysis – an intuitive analysis is enough (8 marks)

2 (a) Explain what is meant by the term 'sanitised information' (6 marks)
(b) What inference problems do you see in applying a 'no read up' access policy at the level of an individual column in a database? (6 marks)
(c) Consider a database that provides a 'no write down' access policy at a granularity of row. What options are available if a user wishes to insert a row with a key that already exists but at a higher clearance than the user possesses? (8 marks)

3 (a) In the context of public key cryptography, what is meant by the terms 'public key' and 'private key' (6 marks)
(b) Could authentication and confidentiality be maintained between two parties through the proper use of two public and two private keys? (6 marks)
(c) In the context of steganography, suggest any two ways that information can be hidden in an image. Given a 24 bit image with three colours (RGB), estimate how much information can be hidden using a least significant bit technique (8 marks)

4 (a) Explain what is meant by 'two factor' and 'three factor' authentication (6 marks)
(b) Explain what is meant by 'rainbow table' and 'dictionary' hash attacks (6 marks)
(c) In the context of ATM security and two factor authentication, outline any two attacks with which you are familiar. What steps would you recommend to be taken in order to lessen the likelihood of their success? (8 marks)

5 (a) Explain why log files are important in forensic work (6 marks)
(b) “The arrival of SSD has made imaging more problematic”. Is this the case? (6 marks)
(c) You are presented with a company laptop that has several encrypted files that an employee refuses to decrypt. Outline several steps that you might take in order to address this situation (8 marks)

6 (a) Explain what is meant by 'DNS cache poisoning' (6 marks)
(b) Explain what is meant by 'ARP cache poisoning/ARP spoofing' (6 marks)
(c) Discuss how Transport Layer Security (TLS) might help in certain circumstances with DNS cache poisoning (8 marks)

7 “A new threat landscape is emerging with super/smartphones and tablets”.
Discuss this statement. (20 marks)